

REMARKS

Favorable reconsideration of this application, in light of the preceding amendment and the following remarks, is respectfully requested.

Claims 17-36 are currently pending in this application, of which claims 17 and 36 are the independent claims, and the remainder dependent. Claim 36 is newly added. Claims 18-19 are currently amended.

SUMMARY OF EXAMINER INTERVIEW

Initially, Applicants thank Examiner Wright for his time during the interview of June 28, 2010. The interview was conducted over telephone between Examiner Wright and the Applicant's Representative.

The merits of the case and how the claimed invention differentiates over the prior art of record was discussed during the course of the interview. Particularly, Applicant's Representative discussed the arguments filed June 7, 2010, explained the example embodiments disclosed in FIGS. 1-4, claims 17-19 and how the claimed invention is distinguished over the prior art of record.

The instant amendment is based on the discussion during the interview. Applicants respectfully request the Examiner kindly reconsider his rejections in view of the interview and the reasons given below.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 17-35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over EP 0 537 971 B1 to Hardy et al. ("Hardy") in view of WO 00/30319 to Kupka et al. ("Kupka") and further in view of U.S. Patent No. 6,507,907 to Takahashi et al. ("Takahashi"). Applicants respectfully traverse this rejection for the reasons detailed below.

Initially Applicants submit that none of the references, Hardy, Takahashi and Kupka, teach or fairly suggest any data exchange method between devices locally connected to one another. For example, Hardy's directed to remote communication between several devices showing several different algorithms. Takahashi is directed to remote communication between two receivers and local communication between the POD module and the host device. As is seen in FIG. 1A of Takahashi the POD module 26 and the host device 28 are both contained in a receiver 20. Kupka is directed to remote communication between a provider and a memory. As such, none of the references teach or fairly suggest *any* "data exchange method between devices locally connected to one another a first device of the two devices being a security module and a second device of the two devices being a receiver," as recited in independent claim 17.

Also, Hardy teaches encrypting random numbers using only public keys. Hardy does not teach or suggest using "asymmetric keys" to encrypt the random numbers, as required by independent claim 17. See, Hardy, column 7, lines 4-5.

Claim 17 recites "the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment."

Acknowledging the deficiencies of Hardy in teaching each and every limitation of claim 17, the Examiner relies on Kupka to cure the noted deficiencies of Hardy. Particularly, the Examiner alleges at page 4 of the Office Action that page 18, lines 5-25 of Kupka disclose the above mentioned limitation of independent claim 1.

In FIG. 6, Kupka illustrates the process of obtaining a unique identifier of the media or building a compound key. As mentioned in Kupka, at step 306 user information is obtained this information is temporarily stored in RAM 64. At step 308 the compound encryption/decryption key is built from the input user information that was temporarily stored in RAM 64 and this compound

encryption/decryption key is stored in RAM 64. However, this compound encryption/decryption key is not a private key. Also, the compound encryption/decryption key is not initialized in any security module. The RAM 64 of Kupka is not a "protected environment." Further, the RAM 64 only temporarily stores (volatile) in the compound encryption/decryption key. However, the "first encrypting key" of claim 17 is required to be stored in a non-volatile memory. *See, application as filed, page 3, line 28.* Furthermore, the compound encryption/decryption key of Kupka does not encrypt/decrypt any random number. The compound encryption/decryption key of Kupka is used to encrypt copy-protected data and not a random number.

For at least these reasons Applicants submit that Kupka fails to disclose or fairly suggest "the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment," as recited in independent claim 17.

Acknowledging the deficiencies of Hardy and Kupka in teaching each and every limitation of independent claim 17, the Examiner relies on the teachings of Takahashi to teach "the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment," as recited in independent claim 17.

FIG. 5 of Takahashi illustrates an entity authentication and key derivation process to protect communication between the host 24 and the POD module 26. In Takahashi, a trusted **third party** supplies a list of device identifiers and corresponding secret keys. These secret keys supplied by the trusted third party 112 are used for a protected communication between the host device 24 and the POD module 26. As is seen in FIG. 1A and is understood from the related disclosure, the host device 24 and the POD module 26 are both on the receiving site 12 of Takahashi. Accordingly the sacred keys of Takahashi cannot facilitate

and/or be used for communication between “two devices locally connected to one another, **a first device of the two devices being a security module and a second device of the two devices being a receiver,**” as required by independent claim 17. For at least all these reasons, Applicants submit that Takahashi fails to overcome the noted deficiencies of Hardy and Kupka. Therefore, the alleged combination of Hardy, Kupka and Takahashi fails to render the limitations of independent claim 17 obvious to one of ordinary skill in the art. (Emphasis Added)

It is alleged in the Office Action at page 4 that Hardy teaches “a session key” as required by independent claim 17. Particularly, the Examiner alleges that Hardy teaches combining of first and second random numbers to form a third random number. In Hardy, the third random number is used as a traffic key for the selected key generator for both terminals. However, Hardy does not disclose or even suggest that the traffic key is used as a “session key” as required by independent claim 17. Namely, Applicants submit that the traffic key of Hardy does not “encrypt and decrypt all or part of the exchanged data between the first and second devices,” as required by independent claim 17. Kupka and Takahashi fail to overcome the noted deficiencies of Hardy. Therefore, the alleged combination of Hardy, Takahashi and Kupka fails to render the limitations of independent claim 17 obvious to one of ordinary skill in the art.

In response to the Applicant’s previously filed amendment, the Examiner alleges on page 12 of the Office Action that Takahashi explicitly discloses using session key to encrypt and decrypt communication.

Column 2, Line 41 of Takahashi discloses a cryptographic technique that uses a session key to encrypt communication. However, nothing in Takahashi discloses or even fairly suggests that this session key of Takahashi is generated by “combining a first and second random number,” as required by independent claim

17. For at least this reason Applicants submit that Takahashi fails to disclose or fairly suggest "session key" as required by independent claim 17.

With respect to the Applicant's previously filed amendment, the Examiner alleges on page 11 of the Office Action that the abstract of Hardy discloses "using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device," as required by independent claim 17. However, the traffic keys are only used to initialize key generators. Hardy is silent with regards to any encrypting or decrypting of data exchanged between the first and second devices.

With respect to dependent claim 18, the Examiner alleges that Hardy in column 7, lines 50 to column 8, lines 5, teaches conducting communication based on comparison of random numbers.

However, the cited sections of Hardy are directed to a method of key generator (KG) synchronization using linear feedback shift registers (LFSR). These sections of Hardy do not deal with encrypting any random numbers (LFSR's are initialized using a seed value or a starting value, and this seed value is user defined. Any values generated by the LFSR during operation can be accurately determined. LFSR's do not function based on random numbers) using encrypting keys and transmitting the encrypted random numbers between devices. Namely, Hardy fails to teach or fairly suggest each and every limitation of dependent claim 18. Kupka and Takahashi fail to overcome the noted deficiencies of Hardy.

For at least all of the above reasons, Applicants submit that Hardy, Kupka and Takahashi, alone or in combination with each other fail to render the limitations of independent claim 17 obvious to one of ordinary skill in the art.

Claims 18-35, dependent on independent claim 17, are patentable for the reasons stated above with respect to claim 17 as well as for their own merits.

Applicants, therefore, respectfully request that the rejection to claims 17-35 under 35 U.S.C. § 103 be withdrawn.

NEW CLAIM

Claim 36 is newly added, and is allowable over Hardy, Kupka and Takahashi at least for the reasons given above with respect to claims 17-18.

CONCLUSION

In view of the above remarks, the Applicants respectfully submit that each of the pending rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to contact the undersigned.

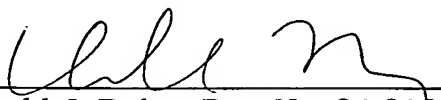
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By


Donald J. Daley, Reg. No. 34,313
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

DJD/AZP:lfb